Senator Al Franken's Opening Statement

(as prepared for delivery)

Mr. Chairman, I want to thank you for holding today's very important hearing. You know, you and I were here together—just two years ago—discussing the security risks associated with vast databases of consumer information like those compiled by data brokers like Equifax. We spoke of such companies as being the perfect target for cyber criminals, and we discussed the lack of accountability that data brokers have to the Americans whose very sensitive information they collect, analyze, and share on a massive scale.

We also talked about the worst case scenario. What happens when there is an unprecedented breach of a company that trades on the information of people with whom they have no direct relationship, and no particular set of obligations?

Well, unfortunately, we all know that we're here again today because that worst case scenario is our new reality.

Because of the gross failures of Equifax, as well as a lack of safeguards protecting our privacy and security, 145 million Americans—including over two million Minnesotans—are facing the risk of identity theft for the rest of their lives. From tax fraud and medical identity theft to even driver's license theft, the threats to individuals' financial security—and frankly, their livelihoods—are too numerous to count and will persist for decades.

To make matters worse, the Americans who could be hit the hardest are the ones who may be least able to bear such a burden. According to a Department of Justice survey, the average victim of identity theft loses $1,343 in stolen assets and expenses. That's money out of Americans' pockets for Equifax's failures, and it's a significant burden for most Americans.

And let's not forget—or downplay—what this breach means for our national security. Whether a foreign power was actually behind the cyber attack on Equifax, there's no longer any doubt that a hostile

foreign government could use the exposed information to target Americans for blackmail or influence future elections.

Mr. Smith, I know you're about to tell us how sorry you are, and I'm sure you've had a lot of sleepless nights in recent months. But as a business that has consistently operated with little to no regard for the well-being of American consumers, I'm wondering whether you—and the rest of Equifax's leadership—foresaw the gravity of a breach and failed to take the proper precautions because you simply don't care. And because you don't have to care. Equifax won't be losing any business as a result of its failures. American consumers are not able to walk away and take their business—or their personal information—elsewhere. And that's because those consumers aren't actually your customers; they are your product. And you've been treating them as such for years.

Perhaps that's why the three big credit bureaus are numbers 2, 3, and 4 in the CFPB's consumer complaint database – trailing behind only Wells Fargo. According to a 2012 FTC report, one in five credit reports contains an error, but for years, consumers have struggled to meaningfully correct that information. And just this year, Equifax settled with the CFPB for ripping off consumers over its website claiming to offer "free" credit scores when in actuality they were signing up for $16 per month subscription service.

Mr. Smith, your disregard for consumers was particularly evident in the first days following disclosure of the breach, when Equifax attempted to force harmed individuals into arbitration and insisted on charging consumers to freeze their credit – practices that were changed only after massive public outcry.

So, today's hearing is an opportunity to get to the bottom of what Equifax didn't do that it should have done, but also to think carefully about the future of data brokers and the credit reporting industry more broadly. Can data brokers with massive troves of data ever fully guarantee the security of that data? And if not, should such entities even exist? And if they must, how do we secure both transparency and accountability from the companies that trade on the most intimate details of our lives.

I look forward to the testimony of our three witnesses. Thank you, Mr. Chairman.